



# Notes from the Community

Editors: Mary Baker ■ HP Labs ■ [mary.baker@hp.com](mailto:mary.baker@hp.com)  
Justin Manweiler ■ IBM T. J. Watson Research Center ■ [jmanweiler@us.ibm.com](mailto:jmanweiler@us.ibm.com)

## Technology Tackles Safety, Eavesdropping, and Student Life

Mary Baker, HP Labs

Justin Manweiler, IBM T.J. Watson Research Center

Thank you for reading this quarter's edition of Notes from the Community. Recent contributions to our Reddit community focus on personal safety, data privacy, home listening devices, smartphone recycling, student life, and two futuristic projects.

### TECHNOLOGY TO THE RESCUE

Device miniaturization brings us new experiences but also helps address age-old worries. One such worry is the personal safety of those we care about. Readers submitted links about two different approaches to keeping our friends and family safe.

#### Safety Jewelry

It seems like a great solution to pin an alarm button to family members who live alone or walk through an empty parking garage after work. But what if those you're trying to protect care more about fashion? How will you get them to wear an alarm?

Long-established companies, such as MedicAlert ([www.medicalert.org](http://www.medicalert.org)), have already solved this problem for static medical warnings by turning the

bracelets into jewelry. Unfortunately, for active alarms, such as the Life Alert necklace ([www.lifealerthelp.com](http://www.lifealerthelp.com)), the "jewelry" still looks like wearable hospital equipment.

Sense6 Design solves this problem by disguising the alarm button in an accessory called the Artemis ([www.artemisfashion.com](http://www.artemisfashion.com)). Tap three times on the Artemis pendant (see Figure 1), and it sends an alarm to a private security company and the potential victim's loved ones. The embedded sensing and communication device fits into your choice of a silver, gold, or diamond-studded palladium necklace pendant or a no-nonsense clip, both of which are shower proof. If the rather bulky pendant isn't your style, future options appear to include a large flat necklace or clunky bracelet. Maybe eventually something more delicate will be possible. For more information, see [www.psfk.com/2014/11/artemis-stylish-smart-jewelry.html](http://www.psfk.com/2014/11/artemis-stylish-smart-jewelry.html).<sup>1</sup>

#### iPhone Home—Or the Police

A second approach is to attach an alarm to something most people already have handy: their smartphones. Lifeshel has

created a case called the Whistl that fits over a smartphone and has buttons on the outside of the case. If you press those buttons, the case emits a very loud sound (120 decibels) and starts up a strobe light. The case also talks to the phone via Bluetooth and causes it to send a distress notification to the police and your choice of pre-programmed contacts. It even causes the phone to start up video and audio recordings so there may be some helpful clarity about the incident afterward.

Of course, none of this is useful if the phone is in the bottom of a purse



Figure 1. The Artemis safety pendant. (Source: Sense6 Design; used with permission.)

### JOIN OUR SUBREDDIT

This column offers a summary of interesting news and research in pervasive and mobile computing, with content drawn from submissions to a shared community on the social news site Reddit, at [www.reddit.com/r/pervasivecomputing](http://www.reddit.com/r/pervasivecomputing). We encourage you to join our subreddit and spread the news of this site to others, so that together we can build a sustainable online community for all aspects of pervasive and ubiquitous computing.

—Mary Baker and Justin Manweiler

or bag or in an awkward pocket. So now there's an excuse to keep that phone in hand! To read more about the device or the partnerships the company has established with victim-service agencies, see [www.theatlantic.com/technology/archive/2014/11/applying-technology-to-the-problem-of-sexual-assault/382594](http://www.theatlantic.com/technology/archive/2014/11/applying-technology-to-the-problem-of-sexual-assault/382594).<sup>2</sup>

### **SAFETY FOR YOUR DATA TOO**

Now that we've strapped on a variety of personal safety devices, we can pause to consider the safety of our data as well. With almost ubiquitous sensing, there are countless opportunities for sensitive data to escape our control. Readers brought our attention to two articles. The first describes privacy issues with self-tracking gadgets and apps. The second suggests that if we're going to put personal data out there, we should be compensated for it.

#### **Your Quantified, But Not Very Private, Self**

The Quantified Self or Lifelogging movement has generated many kinds of personal tracking. There are now gadgets and applications for us to track our physical activities, fitness, diet, sleep habits, alcohol and drug consumption, social interactions, mood, and more. Although having this data available might point out opportunities to improve our health and lives, it can also provide more opportunity for others to access our personal information.

Symantec recently performed a study to determine just how bad the situation really is. They built some relatively simple portable Bluetooth network scanners, walked around with them, and attended sporting events with them. They found that all of the wearable fitness trackers transmitted unique hardware addresses that allowed Symantec's scanners to track the location of the devices—and thus the location of those wearing the products. They also found that 20 percent of tracking applications failed to encrypt user credentials before transmitting them to the cloud,

leaving personal data vulnerable, even when stored in password-protected individual accounts. More than half of the self-tracking apps didn't even have privacy policies. To read more about the Symantec study, its findings, and its suggestions to prevent others from tracking your trackers, see [www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/how-safe-is-your-quantified-self.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf).<sup>3</sup>

#### **Payment for Your Lack of Privacy**

We frequently see stories about governments and large companies gathering comprehensive personal information about us, sometimes without our knowledge. Companies monetize this information by selling it to others or using it themselves for targeted advertising. Quartz ([qz.com](http://qz.com)) recently reported on companies that now consider your personal data so valuable they're willing to pay you for more of it. While the long-established Nielsen ratings and supermarket loyalty cards already offer money or product discounts for data, this move to enrich online data gathering is still somewhat experimental, and pricing is likely to change. To hear more about this opportunity to give up your privacy for money, see <http://qz.com/257950/a-new-way-to-track-your-data-with-your-permission-and-for-a-fee>.<sup>4</sup>

### **MORE FUN WITH PHONES**

Contributors to our subreddit brought our attention to three articles featuring smartphones. Two of these cover yet more data we can use our phones to sense—both cosmic and personal. The third article is all about what to do with our phones as they get old.

#### **Your Phone and Cosmic Rays**

We use our smartphone cameras to take pictures of Halloween costumes, our feet on vacation, crimes in progress, what we cooked last night for dinner, the pool our friends fell into, and of course cute kittens and hedgehogs. Some physicists at UC Irvine and UC

Davis hope to expand our photographic horizons by asking us to take pictures of ultra-high energy cosmic rays as well.

In a project reminiscent of SETI@home, the Crayfis (Cosmic RAYs Found In Smartphones) project aims to use smartphones around the world as a large-scale ground detector array. Air showers generated by cosmic rays create high-energy particles detectable by the CMOS sensors in our phone cameras. These sensors are small and inefficient, but there are potentially a lot of them—over 1.5 billion—to make up for that. Our phones also come equipped with GPS and network connections to label and upload the sensed data. If you're interested in being an astrophysicist, join their collaborative project by checking out <http://crayfis.ps.uci.edu/about.html> or read the team's paper at <http://arxiv.org/pdf/1410.2895v1.pdf>.<sup>5</sup>

#### **Everything about College Students**

While physicists are sensing cosmic rays with smartphones, researchers at Dartmouth College, the University of Texas at Austin, and Northeastern University are sensing students—everything about them. The StudentLife Study used the smartphones of 48 Dartmouth undergraduate and graduate students over a college term (10 weeks) to gather information about the students' mental health, physical activity, sleep habits, social activity, eating habits, academic performance, and reactions to academic workload over the course of the term (see Figure 2). The collected data is rich, detailed, and very personal. For example, it includes location information, conversational information, and data about grades.

Going forward, the team hopes to add feedback and intervention to the phone app to help students live healthier lives, get better grades, and stay safe. One interesting finding is that there was no correlation between the students' class attendance and grades—just knowing that should reduce stress for some students! For more information about the study, see <http://studentlife>.

## NOTES FROM THE COMMUNITY

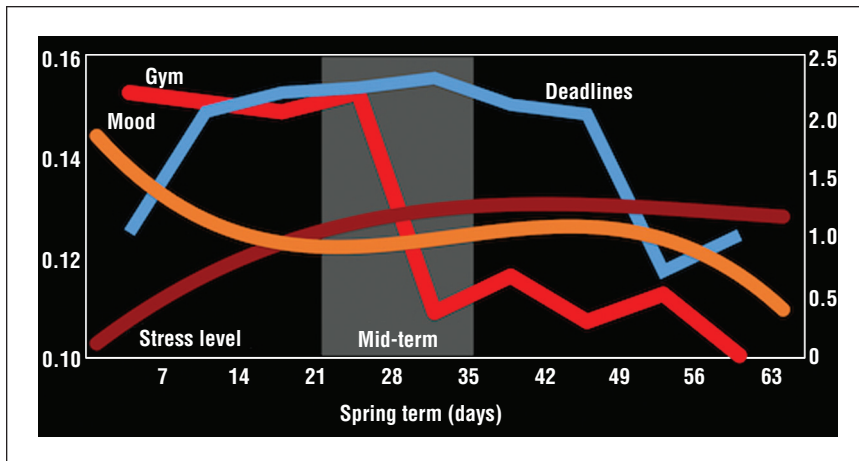


Figure 2. A chart from the StudentLife Study shows that things generally are grim from midterms to the end of the term. (Source: Rui Wang; used with permission.)



Figure 3. Homey listens to your home automation commands. (Source: Homey; used with permission.)

cs.dartmouth.edu. The website includes a link to the anonymized dataset (at least those parts the researchers have been able to anonymize).

### Landfills of Past Sensing and Fashion

The increasing performance and diversity of smartphone sensors should be a good thing, but it has a dark side too. Old phones don't have the sensing capabilities of new phones, and so we give up on them, stick them in drawers, or throw them away. Fashion also plays a role, because many people want to be seen with only the latest gadgets. *Chemical and Engineering News* presents a variety of alarming statistics about smartphone waste, as well

as a description of new projects and chemical processes to help combat the problem.<sup>6</sup>

The world will purchase well over a billion new phones in 2014, but if history is any predictor, owners will give up on most of them after a few years. Alas, only 3 percent of these phones are actually recycled, which is an economic and ecological calamity, especially given the large amounts of precious and poisonous metals in the phones. There's a vastly higher concentration of gold in a phone than in ore from a mine! How is the world trying to address this problem?

Some organizations, such as Project Ara from Google ([www.project-ara.com](http://www.project-ara.com)) are creating more modular phones, so we can replace individual components without throwing away the whole phone. Other organizations are working to make recycling easier, more efficient, and cheaper. One approach, such as that taken by the England-based project Clever (Closed Loop Emotionally Valuable E-waste Recovery; <http://gow.epsrc.ac.uk/NGBOViewGrant.aspx?GrantRef=EP/K026380/1>), is to create phones whose materials are more easily recycled. Other organizations strive toward better chemical processes for recycling existing materials. For example, a new process called

eVOLV might be able to recover up to 98 percent of precious metals in e-waste, and the process can be gradually scaled up in size. Gradual scaling is important, because it allows countries such as Japan, China, and the US (which don't have huge smelting operations) to enter the e-waste recycling fray. Read more on this important topic at <http://cen.acs.org/articles/92/i35/Dialing-Back-Cell-Phone-Waste.html>.<sup>6</sup>

### WHEN THE WALLS HAVE EARS

Audio sensing continues to find its way into more use cases and gadgets. Three submitted links involve audio sensing in the home, each with a different purpose: home automation, security, and ease-of-purchasing.

#### I'll Tell You What to Do

Homey is a home automation hub (see Figure 3) that developers hope will eventually control everything in your home: lights, HVAC, entertainment system, kitchen appliances, and so forth. It is speech controlled, so you'll be able to tell it that when you wake up you want your curtains to open and a ZZ Top album to play at high volume. Most of the functionality seems accessible via a phone app, so you can issue remote commands to ask the oven and hot tub to pre-heat themselves before you get home. Check out this successfully funded project at [athom.nl](http://athom.nl).

#### Loud Sounds in the Night

A Kickstarter project called Point hopes to offer a customizable home security device that is somewhat less invasive than others because it uses audio rather than video. (Apparently, we should feel comfortable with devices listening to us instead of watching us.) The device is a "house sitter" that can send you an alert if it hears a loud sound in a supposedly empty house. It can ask your Airbnb guests ([www.airbnb.com](http://www.airbnb.com)) to turn down the TV late at night. It includes other sensors too, so it will let you know if guests are

smoking inside the house or if humidity levels are so high the walls will grow mold. To read more about this “soft security” device, check out its Facebook page ([www.facebook.com/athomnl/photos\\_stream](http://www.facebook.com/athomnl/photos_stream)) or watch a video at [www.kickstarter.com/projects/830527119/point-a-softer-take-on-home-security?ref=popular](http://www.kickstarter.com/projects/830527119/point-a-softer-take-on-home-security?ref=popular).

### Don't Name your Child Alexa

Perhaps the most curious of the new home-listening devices is the Amazon Echo ([www.amazon.com/oc/echo](http://www.amazon.com/oc/echo)). This black cylinder will sit in your home and listen. If it hears the name Alexa, it will pay attention to what you're saying and do something. You can ask it questions, ask it to perform home automation tasks, and of course, ask it to buy things from Amazon. At the time of writing, the Echo can be purchased by invitation only.

While readers didn't submit a link to the Echo directly, they did submit a link to an amusingly edited version of the Amazon Echo ad. For a small dose of pervasive computing humor, watch <https://www.youtube.com/watch?v=GijLoiVkmYI>. To their credit, Amazon has so far not squelched this parody. It is also the case that we might already have many other listening devices around us in our homes, including smartphones with speech-enabled personal assistants running on them.

### THINGS WE WANT TO PLAY WITH

Large and small, readers point us to systems and gadgets we can't wait to play with.

### Introduction to Circuits


Circuit Scribe is a pen that writes with conductive ink so you can scribble circuits on paper. The kit also comes with various components such as LEDs, power adapters, and buzzers that you can plop down on your circuits to make all sorts of cool things happen. Imagine creating your own wearables with paper, pen, and tape—or origami that



Figure 4. The RoomAlive gaming environment. (Source: Microsoft Research; used with permission.)

does more than look pretty! To see a demo of the pen, check out <http://youtu.be/e0NM1jJbjrM>.

### Gamer's Paradise

As a follow-on from its IllumiRoom research project, Microsoft has combined video projectors and the Kinect to create RoomAlive, a more advanced prototype that extends the Xbox gaming environment to an entire room. The system tracks you throughout the room so you can interact with game objects in the middle of the room or via any of the room's surfaces—walls, floors, and so on. As long as you don't trip over the coffee table, this seems like magic for gamers. Take a look at <http://research.microsoft.com/en-us/projects/roomalive> for more information. 

### REFERENCES

1. C. Stephens, “Stay Safe Yet Fashionable with Artemis Smart Jewelry,” *PSFK*, 14 Nov. 2014; [www.psfk.com/2014/11/artemis-stylish-smart-jewelry.html](http://www.psfk.com/2014/11/artemis-stylish-smart-jewelry.html).
2. J. Tierney, “The iPhone Case That Can Call the Police,” *The Atlantic*, 11 Nov. 2014; [www.theatlantic.com/technology/archive/2014/11/applying-technology-to-the-problem-of-sexual-assault/382594](http://www.theatlantic.com/technology/archive/2014/11/applying-technology-to-the-problem-of-sexual-assault/382594).

3. M.B. Barcena, C. Wueest, and H. Lau, “How Safe is your Quantified Self?” *Symantic*, 11 Aug. 2014; [www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/how-safe-is-your-quantified-self.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf).
4. E. Lopatto, “A New Way to Track your Data: With your Permission and for a Fee,” *Quartz.com*, 2 Sept. 2014; <http://qz.com/257950/a-new-way-to-track-your-data-with-your-permission-and-for-a-fee>.
5. D. Whiteson et al., “Observing Ultra-High Energy Cosmic Rays with Smartphones,” *ArXiv.org*, 10 Oct. 2014; <http://arxiv.org/pdf/1410.2895v1.pdf>.
6. A. Scott, “Dialing Back On Cell Phone Waste,” *Chemical & Engineering News*, vol. 92, no. 35, 2014, pp. 30–33; <http://cen.acs.org/articles/92/i35/Dialing-Back-Cell-Phone-Waste.html>.

**Mary Baker** is a senior research scientist at HP Labs. Contact her at [mgbaker@hp.com](mailto:mgbaker@hp.com).

**Justin Manweiler** is a researcher at the IBM T.J. Watson Research Center. Contact him at [jmanweiler@us.ibm.com](mailto:jmanweiler@us.ibm.com).



Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.